# EOSDIS Element Name

## INFORMATION TECHNOLOGY (IT)

## RISK MANAGEMENT PLAN
## (TEMPLATE)

**Organization Title and Code**

**Month, Year**

**Administratively Controlled Information**

| |
|---|
| This document contains sensitive information and shall be handled in a way that precludes its disclosure to the general public and limits its circulation. NASA entities must attach the NASA Form 1686, Administratively Controlled Information (ACI) form to the cover of this document. |

# EOSDIS Element Name

## INFORMATION TECHNOLOGY (IT) RISK MANAGEMENT PLAN (TEMPLATE)

**Organization Title and Code**

**Prepared by:**

(Name) Date
(Title)
(Organization)

**Reviewed by:**

(Name) Date
(Title)
(Organization)

**Approved by:**

(Name) Date
(Title)
(Organization)

This page intentionally left blank

# Preface

Proposed changes to this document shall be submitted to the ESDIS Computer Security Official (CSO) along with supporting materials justifying the proposed revision. These changes will be issued by Documentation Change Notice (DCN), or where applicable, by complete revision.

Questions concerning this document and proposed changes shall be addressed to:

Clayton Sigman
GSFC, NASA
Greenbelt, MD

# Change Information Page

| Issue | Date | Pages Affected | Description |
|---|---|---|---|
| Original | | | |

This page intentionally left blank

# List of Affected Pages

| Page No. | Revision | Page No. | Revision | Page No. | Revision | Page No. | Revision |
|---|---|---|---|---|---|---|---|
| | | | | | | | |

This page intentionally left blank.

# Table of Contents

# Section 1. Introduction

## 1.1 Purpose

The risk assessment process is a structured process that helps the line manager determine security vulnerabilities detected on project systems. This process further enables the manager to identify various threats that could put his/her system at risk, assess the impact of identified risks to the systems, and determine which risks are acceptable.

## 1.2 Scope

This Risk Management Document identifies all known vulnerabilities residing on Information Technology (IT) assets at **(EOSDIS element name).** Completion of this risk assessment satisfies the Federal security requirement identified in the Office of Management and Budget (OMB) Circular No. A-130, Appendix III. This phase of the EOSDIS Risk Management Program is to satisfy immediate project compliance with the NPG 2810.1 security policy.

## 1.3 Definitions

1 Asset -IT resources found within the element manager's area of responsibility.

2 Element - An EOSDIS facility that generates, archives, and distributes EOS Standard Data Products, and related information, for the duration of the EOS mission. An EOS Element is managed by an institution such as a NASA field center or a university, under terms of agreement with the EOSDIS Project

3 Element Manager -The individual responsible for the overall operations of the EOSDIS element facility.

4 Information Technology (IT) - Hardware and software operated by a Federal agency or a contractor of a Federal agency or other organization that processes information on behalf of the Federal government to accomplish a Federal function, regardless of the technology involved, whether by computers, telecommunications systems, automatic data processing equipment, or other.

5 IT Resource - Hardware, software, network, media, or information within the element manager's area of responsibility.

6 Risk – The results or effects of a threat occurring to an organization. It is the possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.

7 Threat - Any event or circumstance, whether internal or external, deliberate or unintentional, which has the potential to cause harm to a system or to its associated applications or information.

8 Vulnerability – A flaw or weakness that may allow harm to occur to an automated information system or activity.

## 1.4 Applicable Documents

- Office of Management and Budget (OMB) Circular No. A-130, Appendix III

- National Institute of Standards and Technology (NIST) Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook"

- NASA Procedures and Guidelines, Security of Information Technology, NPG 2810. 1, dated August 26, 1999

# Section 2. Data Distribution Facility

## 2.1 Purpose

Identify the purpose of the EOSDIS Element undergoing the Risk Assessment.

## 2.2 Description

Provide a graphic overview of the systems for which this risk management plan is being conducted. Include diagrams of the data flow, the external interfaces, and the systems and network configuration.

# Section 3. Asset and Value Identification

The risk analyst must identify the assets at risk. Assets are those IT resources found within the element/line manager's area of responsibility. Hardware, software, networks, media, and information are among the assets to be considered. Information may be the primary asset at risk and more valuable than the systems and software that process it. Therefore, it is imperative that the nature of the information and its value be known at the outset. The nature of some information, such as personal information, proprietary data, trade secrets, and procurement data, require protection even if it is difficult to place a dollar figure on its value. Knowing the costs associated with replacing or reconstructing IT resources is important in conducting a risk assessment. The following guidelines for determining the value of different resources:

- Hardware - the cost of replacing the functionality, including the physical environment if necessary, of these assets.
- Software applications - an estimate of the cost to rewrite the software or the cost to replace the software.
- Information - an estimate of the cost to retrieve or reconstruct the information. Since the value of some information may decrease over time, it is important to factor the time criticality of information into the estimate.

## 3.1 Asset and Value Identification

***Sample3.1***

**Asset Worksheet**

Location: Bldg. 556, Room 32

| Hardware | Purpose | Replacement Cost | Information Category |
|---|---|---|---|
| 1. MICRON 2550<br>a. OS: Windows NT 4.0<br>b. Office 2000 Pro<br>c. McAfee VirusScan 4.1<br>d. Eudora Gold 3.2<br>Information: EOSDIS programming | Server | 1200.00<br>3500.00<br>892.00<br>80.00<br>40.00<br>250.00 | SER |
| | | | |
| | | | |

*Information Category: Additional information to assist in determining appropriate categorization can be found in the NPG 2810.1.*

MSN - Mission Essential Information
BRT - Business and Restricted Technology
SER - Scientific, Engineering, and Research
ADM – Administrative
PUB - Public Access

## Asset Worksheet

Location:

| Hardware | Purpose | Replacement Cost | Information Category |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

*Information Category: Additional information to assist in determining appropriate categorization can be found in the NPG 2810.1.*

MSN - Mission Essential Information
BRT - Business and Restricted Technology
SER - Scientific, Engineering, and Research
ADM - Administrative
PUB - Public Access

# Section 4. Threats and Impact Identification

This step identifies the threats to the assets at risk. Threats are any events or circumstances, whether internal or external, that have the potential to cause harm to a system or to its associated applications or information. A threat could result in the destruction or modification of the computer systems, networks, software applications, or information; the unauthorized disclosure of information; or the denial of the service that the assets are intended to provide. Threats can be placed into three categories: Environmental; Human unintentional; and Human intentional. Risk is the probability of a threat to occur.

The analyst conducting the risk assessment should list all known threats without regard to their probability of occurrence. The risk assessment should not proceed until the analyst conducting the assessment is satisfied that a comprehensive list of potential threats has been obtained. Make the list of threats as inclusive as possible by doing the following:

- Conduct a walk-through of the facilities.
- Contact the IT Security Manager's Office for current information on intruder attacks.
- Review bulletins regarding security weaknesses of equipment, operating systems, and technologies that are incorporated in this particular system or application.
- Review threats identified by other risk assessments for similar systems at the same location.
- Identify single points of failure in the functional design.

## 4.1 Threats

This worksheet is designed to identify threats and evaluate the probability of occurrence. It can later assist the element/line manager in risk mitigation through contingency planning and creation of administrative and technical controls for their systems.

### Environmental

| Threat | Probability (Hi/Med/Low) | Threat | Probability (Hi/Med/Low) |
|---|---|---|---|
| Aging Facilities | | Leaking Liquids | |
| Air Conditioning Failure | | Lightning Storm | |
| Airborne Particles (Dust) | | Nuclear Mishap | |
| Chemical Spill | | Power Fluctuation | |
| Dirt | | Static Electricity | |
| Earthquake | | Storms (Snow, Ice) | |
| Electro-Magnetic Interference | | Tornado | |
| Explosion | | High Temperatures | |
| Fire (External) | | Time (Aging Media) | |
| Fire (Internal) | | Volcanic Eruption | |
| Flooding | | Other: | |
| Humidity | | Other: | |

## Human Unintentional

| Threat | Probability (Hi/Med/Low) |
|---|---|
| Equipment Failure | |
| Heating Units | |
| Lost Documentation | |
| Lost Encryption Keys | |
| Magnetic Fields | |
| Programmer Error | |
| Spilled Beverages | |
| User Error | |
| Other: | |

## Human Intentional

| Threat | Probability (Hi/Med/Low) |
|---|---|
| Arson | |
| Computer Viruses | |
| File Sabotage | |
| Hacking | |
| Theft | |
| Vandalism | |
| Unauthorized Copying | |
| Wire Taps | |
| Other: | |

# Section 5. Vulnerability and Risk Determination

Vulnerabilities are the mechanisms by which threats access your system. Consider vulnerabilities to natural threats and both intentional and unintentional manmade threats as identified in the previous step. Next, organize the list of vulnerabilities you've generated into categories such as the following and then once again see if additional thoughts come to mind:

- Physical concerns (e.g., room access, building construction, and climate)
- Hardware and software-related issues (e.g., equipment, programs, )
- Media liabilities (e.g., disks, tapes, hard drives, and print copies)
- Communications (e.g., access points and encryption)
- Human concerns (e.g., personnel and office behavior)

The following happens in the typical office quite frequently:

- A door is propped open and doesn't have a lock
- A cup of coffee is set on a computer case.
- A computer monitor sits within plain sight and easy reach of a window.
- Wiring is in the way of foot traffic.
- Equipment is plugged into wall sockets without a surge protector.
- Outlets are overloaded.
- Backup files are stored in the same room as the original files.
- Floppy disks are shared haphazardly and are not labeled.
- Someone's password is written and posted on their monitor.
- A computer is logged on but has been left unattended.

The risk analyst must list and describe the potential vulnerability. For example, if the component is a server containing Privacy Act data, one of the threats might be physical access to the equipment. The vulnerabilities might include the following:

- The system design calls for the server to be placed in an open office area.
- The area proposed for the location of the server is not locked, but it is typically staffed 24 hours per day.
- The server will contain information restricted from unlimited public disclosure, but the area is open to visitors who are escorted at all times.

This step is to determine whether a system is vulnerable to the threats previously identified and in what ways it is vulnerable. If a system or application is vulnerable to a threat, it is considered a risk. The relationship among threats, risks, and vulnerabilities is important. A risk is nothing more than a threat to which the system is vulnerable. If there is no vulnerability, regardless of the seriousness of the threat, there is no risk. If there is no threat, regardless of the seriousness of the vulnerability, there is no risk.

## 5.1 Vulnerability and Risk Determination

This worksheet is designed to identify vulnerabilities of the system's hardware, software and information. The risk analyst assigned to determine the vulnerability to threats should investigate the following:

- Independent audit reports that have been conducted on the system or upon similar systems
- Interviews with system management and development, operations, and maintenance personnel
- Results of penetration tests conducted on the system or on similar systems can be used to identify uncorrected vulnerabilities.
- Information from vendors regarding corrected or uncorrected vulnerabilities of that vendor's systems or software
- Bulletins or other archives of information regarding vulnerabilities of various systems

Vulnerabilities must be documented precisely so they can be addressed in further analysis. For example, "Users frequently write cipher lock combination on the door" is a useful statement of vulnerability, while "Physical controls weak" is not.

When identifying vulnerabilities, analysts should consider any other systems to which the system in question is connected. Since systems are normally interconnected, it is possible that the access provided by another system on the network could result in vulnerability. The analyst should understand any security weaknesses posed by other systems that share common resources.

The analyst should first identify the IT assets (from the worksheet in Appendix A), determine all vulnerabilities, and identify the impact to the asset (either due to the cost of the asset itself or because of the information stored or processed on the asset) if the vulnerability is exploited. The individual should then compare the vulnerability to the threat list (Appendix B) to see if a threat exists which may exploit that vulnerability, and assign the threat probability in the Threat Value column. The last step is to determine the Risk Value by multiplying the Risk Impact and the Threat Value: Low = 1, Medium = 2, High = 3 and None = 0.

***Sample 5.1***

**Risk Determination Worksheet**

**Location:** Goddard Space Flight Center, Bldg 556, Room 32

| Asset Identification | Vulnerability | Risk Impact | **Threat** | Threat Value | Risk Value |
|---|---|---|---|---|---|
| 1. MICRON 2550 | 1. Loss of electricity | High | Environmental | High | 9 |
| | 2. Loss of electricity | High | Human – Unintentional | Low | 3 |
| | 3. Disk crash | High | Environmental | Med | 6 |
| | 4. Leaking fluids | High | Human – Unintentional | Low | 3 |
| | 5. Flooding | High | Environmental | Med | 6 |
| 1a. Windows NT | 6. File sharing violations | Med | Human – Unintentional | High | 6 |
| | 7. File theft | Med | Human – Intentional | High | 6 |
| | 8. Default passwords | High | Human – Unintentional | Low | 3 |

| | | | | | |
|---|---|---|---|---|---|
| | 9. Default passwords | High | Human – Intentional | High | 9 |
| 1b. McAfee VirusScan | 10. Dat files not kept up to date | Med | Human – Intentional | High | 6 |
| 2. CISCO 2550 | 11. Loss of electricity | Med | Environmental | High | 6 |
| 2a. IOS 3.13 | 12. File theft | High | Human – Unintentional | None | 0 |
| | 13. File theft | High | Human – Intentional | High | 9 |

**Risk Determination Worksheet**

**Location:**

| Asset Identification | Vulnerability | Risk Impact | Threat | Threat Value | Risk Value |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## 5.2 Corrected Risk Re-evaluation

The final step in the risk assessment process is to identify controls and processes that are in place that either mitigate or eliminate the vulnerability or threat and determine the new risk level.

***Sample 5.2***

**Corrected Risk Identification Worksheet**

**Location:** Bldg 556, Room 32

| Asset Identification | Vulnerability | Risk Impact | Mitigation Technique | New Risk |
|---|---|---|---|---|
| 1. MICRON 2550 | 1. Loss of electricity | 9 | Generator | 0 |
| | 2. Loss of electricity | 3 | UPS System | 0 |
| | 3. Disk crash | 6 | None | 6 |
| | 4. Leaking fluids | 3 | No drinks allowed | 0 |
| | 5. Flooding | 6 | Room location | 0 |
| 1a. Windows NT | 6. File sharing violation | 6 | All files are password protected | 3 |
| | 7. File theft | 6 | System is behind a firewall | 3 |
| | 8. Default passwords | 3 | Trained administrators/removed | 0 |

| | | | | |
|---|---|---|---|---|
| | 9. Default passwords | 9 | System is behind a firewall | 3 |
| 1b. McAfee VirusScan | 10. Dat files not kept up to date | 6 | Automated update when user logs on. | 0 |
| 2. CISCO 2550 | 11. Loss of electricity | 6 | Generator | 0 |
| 2a. IOS 3.13 | 12. File theft | 0 | | 0 |
| | 13. File theft | 9 | None | 9 |

## Corrected Risk Identification Worksheet

**Location:**

| Asset Identification | Vulnerability | Risk Impact | Mitigation Technique | New Risk |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Section 6. Risk Reduction Analysis

This step identifies the potential controls which can be used to mitigate or eliminate the remaining risks. Some controls are feasible, but implementing them would significantly reduce the ability of the system to function at an acceptable level. Some may be possible to implement, but the life-cycle cost would be excessive.

There is usually more than one way to solve an IT security problem. The analyst's responsibility is to provide cost-effective controls that mitigate, if not fully correct, each of the risks.

1 Technical controls. Those controls provided by the manufacturer of the system or software application as well as third party products. Generally, these controls are inherent in the operating system or application (e.g., the ability to restrict account access or the ability to force password changes at predetermined intervals). These controls are recommended as the first line of defense.

2 Physical controls. Those controls provided by the facility in which the system runs (e.g., a cipher lock for controlling admittance to the facility or access to fire suppression equipment).

3 Procedural controls. Those controls invoked as a result of actions that system personnel take (e.g., required procedures for documenting configuration changes, using sign-in logs, and completing forms or checklists). These controls tend to be the weakest and require management enforcement and continuing training to be effective.

In determining the operational feasibility, the analyst should consider the following:

The system or software application vendor may have already provided a technical control, which might be a matter of invoking an existing option in the operating system or application software. Invoking these controls often results in a cost, usually paid in terms of processing overhead or a reduction in ease of use. The analyst must weigh the benefits gained against the costs.

Physical and procedural controls may be used to supplement or substitute for technical controls. Although it is tempting to view procedural and physical solutions as being "free" since they can often be implemented with existing resources, effectiveness, as well as training, administration, and enforcement costs must be considered.

The physical control of IT resources is extremely important and must be considered in addition to technical and procedural controls.

Each security control has a cost that the analyst must consider before deciding on a recommendation. All three kinds of controls must be balanced to arrive at a comprehensive, cost-effective solution. Costs are paid in various ways. Some costs are paid in dollars, some are reflected in system overhead, and some appear as user inconvenience. The analyst must determine a cost-effective control to mitigate or correct each risk. If no control can be found, then the risk reduction analysis must state this fact.

The analyst may also find security controls available that have no risks or baseline requirements (NPG 2810.1 Appendix A, paragraphs 6 and 7) associated with them.

Before concluding the risk reduction analysis, the analyst must consider any security controls that should be imposed to mitigate risks to those who share common resources

To document the risk reduction analysis, the analyst will annotate the prioritized list of risks with recommended controls for each risk and the cost of implementing each control.

For each uncorrected risk, the analyst must recommend a security control that will either correct the risk or at least mitigate it to the most acceptable extent possible.

## 6.1 Recommended Controls

List the risks from the table in Section 5. Identify what control(s) would mitigate or alleviate the risk, the cost in dollars or overhead to purchase and/or implement the control, and the risk of not implementing that control.

| Risk | Recommended Control | Cost | Impact of Non-Implemention |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

# Section 7. Risk Management

Upon completion of the risk reduction analysis, the analyst will present the recommendations to the manager who is responsible for determining acceptable levels of risk. Because managers are ultimately responsible, they may accept the recommendations as given by the analyst or reprioritize them as necessary. It is not the intent of the NASA IT Security Program to prohibit processing in high-risk situations. The manager must do the following:

- Seek Senior Management and/or legal advice for systems requiring "special management attention" (see NPG 2810.1 special management attention determination) and where the laws or policies apply to the risk decision.

- Decide which recommendations to implement and which risks to accept, based on the realities of budgets, schedules, and deadlines.

- Ensure that, in accepting risks, managers understand the consequences. Managers are within their rights to grant an authorization to process, provided that other systems are not put at risk, as agreed by affected system managers. If managers cannot reach agreement, Senior EOSDIS Project Management will make a determination.

## 7.1 Risk Control Implementation

Describe which controls have been selected from the risk reduction analysis and the expected date of implementation.

***Sample 7.1***

**Management Worksheet**

| Vulnerability | Selected Control/ Comments | Implementation Date |
|---|---|---|
| An expiration date on all accounts is not automatically enforced. | The Unix operating system does not have this capability. However, the system manager will print out a list of all accounts on a monthly basis and verify that they are still current and authorized. Any accounts found not current or authorized will be deleted. This manual review will provide an acceptable level of security regarding account expiration. | 1 Oct 00 |
| There is no contingency/disaster recovery plan. | Develop a Contingency Plan. | 31 Oct 00 |

**Management Worksheet**

| Vulnerability | Selected Control/ Comments | Implementation Date |
|---|---|---|
| | | |
| | | |

## 7.2 Risk Justification for Risks Not Eliminated

Some controls are expensive to implement, and it is appropriate to document and justify why these controls are not being implemented or indicate why they are not applicable. Prioritize the remaining risks by level, high, medium and low.

***Sample 7.2***

**Risk Justification Worksheet**

| Vulnerability | Justification for Acceptance | Level of Risk |
|---|---|---|
| Data being transmitted over networks is not encrypted. | Encryption would require extensive reprogramming of the systems and would also require developing some method to comply with the prohibition of exporting encryption keys to foreign countries. There have been no known instances of violation of data confidentiality using the current method of data transmissions. Encryption is not cost effective. Therefore, not encrypting data is an acceptable risk. | High |
| A user identification is not suspended after five consecutive unsuccessful attempts. | The Unix operating system does not have this capability. The system does record all unsuccessful login attempts. These audit trails are reviewed weekly and no problem in this area has been noticed. Suspending a user ID helps prevent someone from trying to gain access by guessing passwords. The system automatically requires passwords to be changed every 90 days and the CRACK utility is used to check for easily guess-able passwords. These safeguards along with a review of the audit trail provides an acceptable level of security against password guessing. | Medium |
| Access to Building XX after normal business hours is not controlled. | Building XX has minimal external security. The security force locks all external doors at approximately 7 p.m. and unlocks them at 6 a.m. The security force makes patrols of the facility to include Building XX. The ESDIS element on the third floor is staffed 24 hours, 7 days a week, and the doors to the computer room are locked. This provides an acceptable level of physical security to the facility. | Low |

## Risk Justification Worksheet

| Vulnerability | Justification for Acceptance | Level of Risk |
|---|---|---|
| | | |
| | | |
| | | |